UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,335	11/26/2003	Martin Soukup	57983.000166	8387

7590 01/29/2009

Thomas E. Anderson
Hunton & Williams LLP
1900 K Street, N.W.
Washington, DC 20006-1109

EXAMINER	
ZHU, BO HUI ALVIN	
ART UNIT	PAPER NUMBER
2419	
MAIL DATE	DELIVERY MODE
01/29/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/721,335	SOUKUP, MARTIN	
	Examiner	Art Unit	
	BO HUI A. ZHU	2419	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 11-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 11-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The amendment filed on November 19, 2008 has been entered.

Claims 1 – 9 and 11 - 24 are pending.

Claims 1 – 9 and 11 – 24 are rejected.

The 112 1st paragraph rejections of claims 1 – 9, 11 and 22 – 24 have been withdrawn in view of the amendments to the claims.

The 112 2nd paragraph rejections of claims 1 – 9, 11 and 22 – 24 have been withdrawn in view of the amendments to the claims.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3 - 6, 9, 12, 14 – 17 and 20 - 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peng et al. "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring" in view of Kirby et al. (US 5,828,846).

(1) with regard to claims 1, 12 and 21:

Peng et al. disclose a method and system, comprising: receiving a current packet at a first network element (a detection engine receives incoming packets); identifying at least part of a source address of a packet; querying a storage module (a Hash table of

the detection engine) of the network element to identify at least one source address of a previously received packet; determining whether the at least part of the source address of the current packet matches at least part of the at least one source address of the previously received packet (page 4, Section A and Fig. 3. The reference teaches the detection engine matches the IP source address of the incoming packets to the source addresses recorded in a hash table for a time interval Δn); determining whether the at least part of the source address of the current packet matches at least part of the at least one source address of the previously received packet (page 4, Section A; if an address matches one recorded in the hash table, the arrival time of the packet is recorded in the hash table).

Peng et al. does not disclose routing the current packet to a second network element if the at least part of the source address of the current packet matches at least part of the at least one source address of the previously received packet.

Kirby et al. teaches routing a packet to its destination if the source/destination address of the packet matches an entry in a table stored at a router (see column 4, lines 12 - 20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Peng et al. to route the current packet to its destination when the source address of the packet matches an existing entry stored in the hash table in order to prevent attack traffic from being forwarded.

(2) with regard to claims 3 and 14:

Peng et al. further discloses a Last Time Seen (LTS) value associated with each of the at least one source address is recorded (Fig. 3, the most recent time stamp).

(3) with regard to claims 4 and 15:

Peng et al. further discloses recording an arrival time of the packet (page 4, Section A; the arrival time of the packet is recorded in the hash table, and the count for the number of packets having that address is updated).

(4) with regard to claims 5 and 16:

Peng et al. further discloses routing the current packet to the network element with a warning if the at least part of the source address of the current packet does not match at least part of the at least one source address of the previously received packet; and recording the at least part of the source address of the current packet and an reception time of the current packet (page 4, Section A; if the address is not already in the hash table, it is added to it and the arrival time of the packet is recorded; the newly added address in the hash table can be viewed as a warning because the number of the newly added address appeared in a time slot is used to measured if a attack has occurred in the network).

(5) with regard to claims 6 and 17:

Peng et al. does not disclose the warning is recorded in a read-only medium. The Examiner takes Official Notice that the use of read-only medium is well known in the art. It is desirable to use read-only medium to store data because it provides higher security and protection to the data being stored since data stored in a read-only medium cannot be easily modified. Therefore, it would have been obvious to one of ordinary

skill in the art at the time of the invention to use read-only medium to store the warning in the system of Peng et al.

(6) with regard to claims 9 and 20:

Peng et al. further discloses the source address of the packet is an internet protocol (IP) address (page 4, Section A).

(7) with regard to claim 22:

Peng et al. further disclose the at least one source address of the previously received packet is recorded within a predetermined time period prior to receiving the current packet (page 4, Section A and Fig. 3. The reference teaches matching the IP source address of the incoming packets to the source addresses recorded in a hash table for a time interval Δn).

4. Claims 2, 13, 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peng et al. "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring" in view of Kirby et al. (US 5,828,846) and further in view of Hariguchi et al. (US 6,665,297).

(1) with regard to claims 2 and 13:

Peng et al. further discloses the at least one source address is recorded in a hierarchical data structure, wherein the hierarchical data structure is based at least in part on a plurality of classes of subnet (Fig. 3, the hash table records addresses in a hierarchical data structure).

Peng et al. does not disclose the hierarchical data structure is based at least in part on a plurality of classes of subnet.

Hariguchi et al. teaches a routing table that is based at on a plurality of classes of subnet (e.g. see routing table 40; column 5, lines 20 – 31).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Peng et al. so that the hierarchical data structure is based at least in part on a plurality of classes of subnet as taught in Hariguchi et al. in order to improve the efficiency of searching for an specified entry in a routing table and reduce implementation cost.

(2) with regard to claim 23:

Peng et al. does not disclose the plurality of classes of subnet comprises at least one of a class A subnet, a class B subnet, and a class C subnet, wherein the class A subnet comprises a first octet of the at least one source address recorded, the class B subnet comprises a second octet of the at least one source address recorded, and the class C subnet comprises a third octet of the at least one source address recorded.

Hariguchi et al. teaches the plurality of classes of subnet comprises at least one of a class A subnet, a class B subnet, and a class C subnet, wherein the class A subnet comprises a first octet of an address (hash circuit 82-8), the class B subnet comprises a second octet of an address (hash circuit 82-16), and the class C subnet comprises a third octet of an address (hash circuit 82-24).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Peng et al. so that the plurality of classes of subnet

comprises at least one of a class A subnet, a class B subnet, and a class C subnet, wherein the class A subnet comprises a first octet of the at least one source address recorded, the class B subnet comprises a second octet of the at least one source address recorded, and the class C subnet comprises a third octet of the at least one source address recorded as taught in Hariguchi et al. in order to improve the efficiency of searching for an specified entry in a routing table and reduce implementation cost.

(3) with regard to claim 24:

Peng et al. does not disclose comparing the at least part of the source address of the current packet with at least one of the plurality of classes of subnet of the at least one source address of the previously received packet.

Hariguchi et al. teaches comparing at least part of an address of a packet with at least one of the plurality of classes of subnet (e.g. see column 5, lines 6 – 15).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Peng et al. so that the plurality of classes of subnet comprises at least one of a class A subnet, a class B subnet, and a class C subnet, wherein the class A subnet comprises a first octet of the at least one source address recorded, the class B subnet comprises a second octet of the at least one source address recorded, and the class C subnet comprises a third octet of the at least one source address recorded as taught in Hariguchi et al. in order to improve the efficiency of searching for an specified entry in a routing table and reduce implementation cost.

5. Claims 7, 8, 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peng et al. "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring" in view of Lingafelt et al. (US 2002/0147925).

(1) with regard to claims 7 and 18:

Peng et al. further disclose issuing a warning if the at least part of the source address does not match at least part of the at least one source address of the previously received packet (page 4, Section A; if the address is not already in the hash table, it is added to it; the newly added address in the hash table can be viewed as a warning because the number of the newly added address appeared in a time slot is used to measured if a attack has occurred in the network).

Peng et al. however does not disclose discarding the current packet.

Lingafelt et al. teaches discarding a packet if it does not match with an address in a database of addresses (335 in Fig. 3; paragraph [0025]).

It would have been desirable to discard the packet if it does not match an address in a database of addresses because it would improve the security of the system by not allowing unauthorized traffic to access network resources. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to discard the packets that are not authorized as taught by Lingafelt et al. in the system of Peng et al.

(2) with regard to claims 8 and 19:

Peng et al. does not disclose the warning is recorded in a read-only medium. The Examiner takes Official Notice that the use of read-only medium is well known in

the art. It is desirable to use read-only medium to store data because it provides higher security and protection to the data being stored since data stored in a read-only medium cannot be easily modified. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use read-only medium to store the warning in the system of Peng et al.

6. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Peng et al. "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring" in view of Kirby et al. (US 5,828,846) and further in view of Langberg et al. (US 5,852,630).

(1) with regard to claim 11:

Peng et al. discloses all of the subject matter as discussed in the rejection of claim 1. However, Peng et al. does not teach using a processor readable medium stored thereon a computer executable program for performing the method of claim 1.

Langberg et al. teaches a method for a transceiver warm start activation procedure can be implemented in software stored in a computer-readable medium. The computer-readable medium is an electronic, magnetic, optical, or other physical device or means that can contain or store a computer program for use by or in connection with a computer-related system or method (column 3, lines 51-65). Using a computer readable medium with program instruction code would be desirable because it would perform the same function of using hardware but offer the advantage of less expense, adaptability and flexibility. Therefore, it would have been obvious to one of ordinary skill

in the art at the time the invention was made to include the limitation as taught by Langberg et al. into the system of Peng et al. so as to reduce cost and improve the adaptability and flexibility of the logic simulation.

Response to Arguments

7. Applicant's arguments filed on November 19, 2008 have been fully considered but they are not persuasive.

8. Regarding claims 1, 12 and 21, Applicant argues that Peng does not disclose or suggest "querying a storage module of the first network element to identify at least one source address of a previously received packet." (Remarks, page 15) Examiner respectfully disagrees. Peng discloses "adds legitimate IP addresses into an IP Address Database (IAD) and keeps the IAD updated by adding new legitimate IP addresses and deleting expired IP addresses." "a hash table is used t record the IP addresses that appeared in the current time interval." "Every hash table entry contains two fields, the number of IP packets and the time stamp of the most recent packet for that IP address." "By comparing the current counts of the hash table with the IAD, we can calculate how many new IP addresses have appeared in this time slot." So, Peng discloses a previously recorded IP address in the hash table is identified to match an IP address because the hash table records IP addresses, the number of times packets of the same IP address has been recorded, and the time the most recent packet was received.

9. Applicant further argues that Peng teaches away from Kirby and that it would not have been obvious to one of ordinary skill in the art at the time of the invention to utilize the routing control (e.g., specific types of packets) of Kirby in order to calculate a number of new IP addresses that appear in a time slot of Peng (Remarks, pages 17 - 18). Examiner respectfully disagrees. Peng does not teach away from Kirby. Peng teaches using a hash table to record IP addresses that have been received, record new packet of an IP address if the IP address matches an IP address previously recorded in the hash table. What Peng does not disclose is routing the packet to a network element if there is a match of IP addresses. Kirby teaches a packet is routed to a destination when there is a match between an address of the packet and an entry in a table. It would have been obvious for one of ordinary skill in the art at the time the invention was made to modify Peng to route a packet with an IP address that matches an entry stored in its hash table towards a destination.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BO HUI A. ZHU whose telephone number is (571)270-1086. The examiner can normally be reached on Mon-Thur 10am-6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on (571)272-3088. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BO HUI A ZHU
Examiner, Art Unit 2419

/Hassan Kizou/
Supervisory Patent Examiner, Art Unit 2419